GOVERNMENT OF WESTERN AUSTRALIA

PSC Public Sector Commission

# PUBLIC SECTOR COMMISSIONER'S CIRCULAR

**Enquiries To:** ICT Policy, Strategy and Review
6551 1493
Department of Finance

**Number:** 2010-05
**Issue Date:** 16 April 2010
**Review Date:** 31 August 2014

**Supersedes:** Public Sector Commissioner's Circular 2009-26

---

**TITLE: COMPUTER INFORMATION AND INTERNET SECURITY**

---

## POLICY

Agencies are to ensure that they have policies and procedures in place to manage:

- General controls of computer systems;
- The protection of personal and sensitive information;
- Network threats that aid in the spread of viruses and malicious software; and
- Laptops and Portable Storage Devices.

In recent examinations the Auditor General has found weaknesses in the above areas of risk. Appropriate action to address these issues must be undertaken.

## BACKGROUND

On 27 March 2006 Cabinet directed that the Chief Executive Officer of each government agency is responsible for ensuring their agency implements an appropriate level of information and Internet security. In undertaking this responsibility, attention needs to be given to specific areas of weakness identified in the series of Information Systems Audit reports by the Auditor General, and surveys undertaken from time to time by the Department of Finance.

### General Controls of Computer Systems

Agencies are to be proactive in ensuring that general computer, application and database controls are in place, up-to-date, regularly tested and enforced to ensure that the confidentiality, integrity and availability of computer systems and information is not compromised. Computer systems must be configured and monitored to ensure that there is no unauthorised access to or loss of information, and that any fraudulent activity or inappropriate access can be readily detected.

### Personal and Sensitive Information

Agencies are to have a security policy in place that reflects the sensitivity of the information they store. This should include identifying all instances of personal and sensitive information held and, based on risk assessments, ensuring there is an appropriate level of security controls over the information. All users who will be given access to, or who have access to personal and sensitive data must be appropriately authorised. It may also be necessary to undertake screening including completing background and criminal record checks. In addition, users should understand and

have signed appropriate confidentiality and acceptable use of information systems agreements.

Network Threats

Agencies should keep security software up-to-date with the latest recommended updates, and ensure that their systems are patched for known vulnerabilities. Policies and procedures should be in place to govern security software management, software updates, and security in general. As well, security software and other security devices and mechanisms within agencies must have adequate audit trails enabled.

Laptops and Portable Security Devices

Laptop computers, hand held devices and non-standard operating systems that connect into corporate networks, as well as wireless technologies and interconnected networks without protective devices can aid the spread of malicious software infection and introduce vulnerabilities. These require security considerations before allowing connection into the corporate network.

The portability of laptop computers and other portable storage devices (PSDs) – including flash drives, portable hard drives and mobile phones – places them at greater risk of being lost or stolen. The information stored on PSDs needs to be adequately protected. Comprehensive management, technical and physical controls over these devices is needed to minimise the risk of them being lost or stolen and of sensitive information being accessed.

M C Wauchope
PUBLIC SECTOR COMMISSIONER

| Other relevant Public Sector Commissioner's Circulars: | n/a |
|---|---|